

Susan M. Rotkis, AZ Bar 032866  
Consumer Litigation Associates West, PLLC  
382 S. Convent Ave.  
Tucson, AZ 85716  
520-622-2481  
srotkis@clalegal.com

Leonard A. Bennett  
*pro hac vice*  
Consumer Litigation Associates, P.C.  
763 J. Clyde Morris Blvd, Suite 1-A  
Newport News, VA 23601  
757-930-3660  
lenbennett@clalegal.com

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ARIZONA**

**CORINNE COOPER, MORGAN  
RUTHERFORD, DONNA DECONCINI,  
MARY BRADLEY, DEBBIE REINERT,  
RANDY REINERT,**  
*on behalf of themselves and all others  
similarly situated,*

**Plaintiffs,**

**v.**

**EQUIFAX. INC., a Georgia  
corporation, and EQUIFAX  
INFORMATION SERVICES, LLC, a  
foreign limited liability company, and  
EQUIFAX CONSUMER SERVICES LLC, a  
Georgia limited liability company,**

**Defendants.**

**Case No.: 4:17CV490-RM**

**CLASS ACTION COMPLAINT**

1 COME NOW Plaintiffs, Corinne Cooper, Morgan Rutherford, and Donna DeConcini, on  
2 behalf of themselves and all other consumers similarly situated, by counsel, seek judgment against  
3 Defendants Equifax. Inc., Equifax Information Services, LLC (“EIS”), and Equifax Consumer  
4 Services LLC (“ECS”) (collectively, “Equifax”), and state as follows:  
5

6 **I. PRELIMINARY STATEMENT**

7  
8 1. This is an action for damages, costs, and attorneys’ fees brought pursuant to  
9 common-law negligence. Defendants negligently allowed the fraudulent procurement of the  
10 critical private information of class member consumer report files, and failed to disclose the fact  
11 of such procurement from plaintiffs.

12 2. Defendants operate together as a unified consumer reporting agency (“CRA”) to  
13 prepare and furnish consumer reports for credit and other purposes. Equifax’s databases contain a  
14 treasure trove of valuable information about nearly every American adult—account numbers and  
15 payment histories, Social Security numbers, names and aliases, birthdates, addresses, employment  
16 histories, and the like—that Equifax collects and sells to businesses that extend credit, loan money,  
17 sell insurance, and grant employment, among numerous other activities.  
18

19 3. Defendants obtain the largest portion of their vast store of data independently and  
20 without consumers’ consent or knowledge. Put differently, consumers rarely turn data over to  
21 Equifax knowingly and willingly—most of the data Equifax possesses it obtained from sources  
22 other than the consumers themselves.  
23  
24  
25  
26  
27  
28

1           4. By now, the Court well familiar with the “Equifax breach” and, possibly,  
2 Defendant’s response to it including testimony in front of several congressional committees on  
3 October 3, 2017.  
4

5           5. In May of 2017, and likely earlier, unknown individuals electronically accessed  
6 Equifax’s databases without Defendants’ knowledge, gaining access to information about  
7 approximately 145,500,000 Americans.<sup>1</sup> Ironically, the identity thieves entered Equifax’s systems  
8 through the Internet portal it uses to receive consumer disputes of identity theft and other credit  
9 inaccuracies,<sup>2</sup> and then accessed collateral database information from there, including Defendant’s  
10 core consumer contact database, “ACIS.”<sup>3</sup>  
11

12           6. Defendants have disclosed generally that the fraudulent users procured consumers’  
13 names, Social Security numbers, birthdates, addresses, and driver’s license numbers.<sup>4</sup> Thus,  
14 Equifax furnished this information to the fraudulent users. The breach lasted for months and,  
15 although Equifax knew about the security vulnerability in May, and the breach itself in July at the  
16 latest, it sat on this information until September 8, 2017.  
17

18           7. While Equifax has revealed that the breach took place, it has been anything but  
19 transparent. It has yet to identify the specific individuals affected, reveal exactly what information  
20

---

21  
22  
23 <sup>1</sup> See <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>

24 <sup>2</sup> Equifax had created that portal as a means to fully automate its “reinvestigations” of consumer  
25 disputes and – in theory – avoid the expense of having live human beings oversee that process  
and obligation.

26 <sup>3</sup> “ACIS” is Equifax’s acronym for its “Automated Consumer Interview System”.

27 <sup>4</sup> <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832>.

1 was taken or learned by the hackers and when, or take any preventative steps other than to alert  
2 consumers who are able to navigate its website that they “may” be affected by the breach, often  
3 with inconsistent results. For a company that traffics in electronic information of such a sensitive  
4 and specific nature, this is unacceptable.

6 8. Plaintiffs include Arizona and National consumers regarding whom Defendants  
7 possessed information protected by the federal Fair Credit Reporting Act, which was thereafter  
8 unlawfully procured by identity thieves between March and July 2017.

10 9. Plaintiffs assert a negligence claim for themselves and all other Arizona consumers.  
11 Equifax possessed significant, important financial data about them but failed to exercise the  
12 standard of care required of an entity with such “grave responsibilities” that come along with the  
13 right to store and sell such information. 15 U.S.C. § 1681. Because of that failure, Equifax  
14 permitted unauthorized access to Plaintiffs’ and Class Members’ personal information, which in  
15 turn caused them to suffer not only actual harm caused by the stress of not being able to know  
16 what was accessed and how it will be used by the perpetrators of the breach, but also the risk of  
17 harm that their identities will be stolen, accounts improperly accessed, or credit injured, among  
18 other potential harms.

## 21 II. JURISDICTION

22 10. The Court has diversity jurisdiction as to all Plaintiffs and all class members  
23 pursuant to 28 U.S.C. § 1332(a) as all Plaintiffs seek to recover damages in excess of \$75,000  
24 individually for actual damages and every Plaintiff is diverse from Defendants.

13. Defendant Equifax is subject to personal jurisdiction in the District of Arizona, by virtue of the business it conducts in the Division. Further, it deliberately and specifically availed itself of the benefits of Arizona and caused direct injury to Arizona consumers, including the Plaintiffs, in Arizona.

CLASS ACTION COMPLAINT - 5

1           15. Each representative Plaintiff is a natural person. The putative class is comprised of  
2 natural persons, all of whom are consumers as defined by the Fair Credit Reporting Act (“FCRA”)  
3 15 U.S.C. § 1681 et seq.  
4

5           16. Each Plaintiff named herein has reason to believe, based upon the public reports of  
6 the Data Breach, its scale, and upon information provided by Equifax via its website, that his or  
7 her personal identifying information (“PII”) was taken during the Data Breach.  
8

9           17. Plaintiff Corinne Cooper is a resident of Tucson, Arizona. In or about September  
10 of 2017, Ms. Cooper visited the Equifax website which stated to her that she may be a victim of  
11 the Data Breach. Ms. Cooper has devoted significant time to monitoring her accounts in response  
12 to the Data Breach, including by activating credit “freezes” at Equifax, TransUnion LLC, and  
13 Experian Information Solutions, LLC, and Innovis. She has had to pay money to at least one  
14 additional consumer reporting agency to have her credit freeze initiated. She was never alerted or  
15 advised by Equifax that her consumer report information had been procured as a result of the Data  
16 Breach.  
17

18           18. Plaintiff Morgan Rutherford is a resident of Tucson, Arizona. In or about  
19 September of 2017, Ms. Rutherford visited the Equifax website which stated to her that she may  
20 be a victim of the Data Breach. Ms. Rutherford has devoted significant time to monitoring her  
21 accounts in response to the Data Breach, including initiating credit freezes. She was never alerted  
22 or advised by Equifax that her consumer report information had been procured as a result of the  
23 Data Breach.  
24  
25  
26  
27  
28

1           19. Plaintiff Donna DeConcini is a resident of Tucson, Arizona. In or about September  
2 of 2017, Ms. DeConcini visited the Equifax website which stated to her that she may be a victim  
3 of the Data Breach. Ms. DeConcini has devoted significant time to monitoring her accounts in  
4 response to the Data Breach, including initiating credit freezes. She was never alerted or advised  
5 by Equifax that her consumer report information had been procured as a result of the Data Breach.  
6

7  
8           20. Plaintiff Mary Bradley is a resident of Tucson, Arizona. In or about September of  
9 2017, Ms. Bradley visited the Equifax website which stated to her that she may be a victim of the  
10 Data Breach. Ms. Bradley has devoted significant time to monitoring her accounts in response to  
11 the Data Breach. She was never alerted or advised by Equifax that her consumer report information  
12 had been procured as a result of the Data Breach.  
13

14           21. Plaintiff Debbie Reinert is a resident of Tucson, Arizona. In or about September  
15 of 2017, Ms. Reinert visited the Equifax website which stated to her that she may be a victim of  
16 the Data Breach. Ms. Reinert has devoted significant time to monitoring her accounts in response  
17 to the Data Breach. She was never alerted or advised by Equifax that her consumer report  
18 information had been procured as a result of the Data Breach.  
19

20           22. Plaintiff Randy Reinert is a resident of Tucson, Arizona. In or about September of  
21 2017, Ms. Reinert visited the Equifax website which stated to him that he may be a victim of the  
22 Data Breach. Ms. Reinert has devoted significant time to monitoring his accounts in response to  
23 the Data Breach. He was never alerted or advised by Equifax that his consumer report information  
24 had been procured as a result of the Data Breach.  
25

1           23. All three Defendants are both “consumer reporting agencies” and “nationwide  
2 consumer reporting agencies” as defined and governed un the FCRA.

3  
4           24. Defendant Equifax, Inc. is the parent of the two additional Defendants. In prior  
5 litigation, it has taken the position that it is not itself a “consumer reporting agency” governed by  
6 the FCRA. *See* 15 U.S.C. § 1681a(f) (“The term “consumer reporting agency” means any person  
7 which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or  
8 in part in the practice of assembling or evaluating consumer credit information or other information  
9 on consumers for the purpose of furnishing consumer reports to third parties, and which uses any  
10 means or facility of interstate commerce for the purpose of preparing or furnishing consumer  
11 reports.”)

12  
13           25. But of course, Equifax, Inc. *is* a consumer reporting agency. For purposes of the  
14 FCRA, Equifax, Inc. has held itself out repeatedly to consumers, regulators and the public  
15 generally as the actual operating entity. The branding, labels and disclosures on the Defendants’  
16 consumer website is dominated by “Equifax, Inc.” titling. Defendants have held Equifax, Inc. out  
17 as the operating and responsible entity.

18  
19           26. Defendant Equifax Consumer Services, LLC is similarly a CRA. It for monetary  
20 fees, regularly engages in part in the practice of assembling and maintaining consumer report  
21 information in its operational relationship with Equifax, Inc. and EIS.

22  
23           27. Defendant Equifax Information Services, LLC is a foreign limited liability  
24 company transacting business in Arizona and maintains a registered agent office in Phoenix. At  
25  
26  
27  
28

1 all times relevant to this action, EIS has acknowledged that it is and was a “consumer reporting  
2 agency” as defined by the Fair Credit Reporting Act, § 1681a(f).

3  
4 28. The FCRA, through a rule mandated at § 1681x, expressly prohibits “a consumer  
5 reporting agency from circumventing or evading treatment as a consumer reporting agency” by  
6 means of corporate reorganization or structuring.

7  
8 29. Equifax, Inc. and its subsidiaries – whether or not they observe state law corporate  
9 formalities – have eliminated nearly all lines between their different business entities in the  
10 collection, maintenance, sharing and furnishing of consumer reporting information. Equifax, Inc.,  
11 entities such as EIS regularly share FCRA restricted information with sibling entity ECS to market  
12 and profit from the sale of consumer identity theft prevention products, including the blurring of  
13 legal lines between providing file information under the FCRA versus for private sale to the  
14 consumer. Equifax subsidiary TALX Corporation operates as Equifax Workforce Solutions, and  
15 with control of acquired-entity eThority and both provides and obtains FCRA-governed consumer  
16 information to and from other Equifax entities. Equifax entity Anakam, Inc. integrates Equifax  
17 consumer data for sale of its fraud detection and verification products, largely now under the  
18 Equifax brand. And, by last example Equifax Mortgage Services operates as a separate entity  
19 focused on the mortgage services industry, but also freely shares and uses otherwise FCRA  
20 protected data.

21  
22  
23 30. Further, throughout this breach and post-exposure conduct, the Defendants have  
24 operated and acted as one entity and CRA.

1           31. Here, Equifax, Inc. has used EIS and ECS as dependent and integrated divisions  
2 rather than as separate legal entities. The business operations are fully coordinated and shared.  
3 Resources are cross-applied without full and complete cost and profit centers. Management  
4 decisions at EIS and ECS are made by and through management at Equifax, Inc. And the entities  
5 largely hold themselves out as a single uniform business.  
6

7           32. For purposes of the claims here, these facts are especially meaningful. Data  
8 security was shared and the negligence here was directly that of management officials at Equifax,  
9 Inc. In fact, it was Equifax, Inc.'s Chief Security Officer Susan Mauldin and Chief Information  
10 Officer David Webb who Defendants have fired as a result of the events alleged herein, rather than  
11 employees of the subsidiary entities. Equifax, Inc.'s president has directed all matters related to  
12 these events. And Equifax, Inc.'s General Counsel was and has remained the Chief Legal Officer  
13 and compliance official for all Equifax entities as of October 3, 2017. Equifax's Chief Executive  
14 Officer Richard Smith recently resigned, but reportedly was paid \$90 million upon his departure.  
15

16           33. To remain separate and distinct for the purposes of liability in this action,  
17 Defendants must operate as separate and legally as well as operationally distinct entities. Here,  
18 for matters and functions alleged and relevant herein, EIS and ECS were merely alter egos of  
19 Equifax, Inc. For purposes of how consumer data was handled, warehoused, used and sold, the  
20 corporate lines were disregarded in practice. EIS and ECS were mere instrumentalities for the  
21 transaction of the corporate consumer credit business. The Defendants shared full unity of interest  
22 and ownership such that the separate personalities of the corporation and subsidiaries no longer  
23 existed.  
24  
25  
26



1 regulations relating to consumer privacy, data and financial protection. These regulations are  
2 complex, change frequently, have tended to become more stringent over time[.]”

3  
4 38. The standard duty of care for Equifax was significant. It possessed – for profit and  
5 resale – the very private personal identifiers and financial information on nearly every consumer  
6 in the nation. In fact, Equifax possesses significantly greater amounts of that information than  
7 even the Federal and State governments, which themselves have to purchase reporting products  
8 from Equifax to discover such information. The standard for Equifax’s maintenance and  
9 monitoring of its systems is much greater than an ordinary business.  
10

11 39. The Gramm–Leach–Bliley Act (“GLBA”), 15 U.S. Code § 6801, and the  
12 regulations promulgated thereunder also imposed a duty on Equifax to insure the security and  
13 confidentiality of customer records and information, to protect against hazards including  
14 unauthorized access or use, and to notify affected customers as soon as possible of any breach of  
15 security.  
16

17 40. Equifax owed these duties, in particular, to Plaintiffs and Class Members, as  
18 persons whose personal identifying information (“PII”) and other information was in Equifax’s  
19 possession.  
20

21 41. Equifax had a special relationship with the Plaintiffs and Class Members because  
22 it was entrusted with their personal information. Equifax’s ability to acquire Class Members’ PII  
23 and other information from them and other entities, created an independent duty of care because it  
24 was predicated on the understanding, based on Equifax’s own representations, that Equifax would  
25 take adequate security precautions.  
26

1           42. Further, Equifax's trade in the private and critical financial information of  
2 consumers poses an abnormally dangerous risk of financial harm to those consumers.  
3

4           43. EIS is the entity that Equifax uses to warehouse and administer the retail credit  
5 information and credit reporting function for U.S. consumers. It gathers the information from third  
6 parties it labels "subscribers," referred to as "furnishers" under the FCRA, builds files matching  
7 that data to specific consumers and stores it in a database it titles "ACRO."  
8

9           44. Separately, Equifax maintains the ACIS database which includes all documents  
10 created or obtained by Equifax from consumer contacts, such as consumer disputes, requests for a  
11 copy of the consumer's own credit file, correspondence sent to the consumer, and substantial  
12 amounts of data generated to document and archive each of these contacts. Communications that  
13 come in from the Equifax Internet portal that was the conduit for the data breach are maintained  
14 in the ACIS system. And Equifax has tried to convince the public generally that its "core database"  
15 was not breached. But that distinction is meaningless as entry into the ACIS system provides  
16 access to nearly all of the same data – personal identifiers, accounts, etc. – that would be useful  
17 from the ACRO database. And access through ACIS gets a user directly into other data troves  
18 containing comparable information.  
19

20           45. In the modest amount of information that it has released publicly, Equifax admits  
21 that its security team first observed suspicious network traffic associated with its U.S. online  
22 dispute portal web application no earlier than July 29, 2017 and continuing overnight into July 30,  
23 2017.  
24

25           46. Equifax cannot state with any certainty when this intrusion began.  
26



1 was the most critical type of vulnerability known to the developers.

2  
3 55. Notwithstanding that the particular vulnerability in Apache Struts was identified  
4 and disclosed by U.S. CERT in early March 2017, Equifax failed to successfully apply the “patch”  
5 to its systems that would have fixed the problem.

6 56. Between March 7, 2017 and July 29, 2017, Equifax did not successfully apply the  
7 patch, if it even attempted to at all.

8  
9 57. Equifax admits that the unauthorized accesses to certain files containing personal  
10 consumer reporting information occurred between, at least, May 13, 2017 through July 30, 2017.  
11 Equifax is also unable to rule out that the problem may have started even earlier during a separate  
12 successful and similar hack in March 2017 of its payroll subsidiary TALX (responsible for its  
13 “Work Number” payroll information product that Equifax markets to employers and data brokers).

14  
15 58. The information obtained from TALX, particularly W-2 information stolen just  
16 before tax season, was likely a gold mine to those intruders as it allowed them to file false income  
17 tax returns.

18 59. Form W-2 information frequently sells in the range of \$40 to \$50 per individual  
19 between criminals on the internet.

20  
21 60. Following a review by Mandiant, an outside security company that also  
22 investigated the March 2017 TALX breach but somehow still failed to correct this vulnerability,  
23 Equifax concluded that personal information relating to 143 million U.S. consumers – primarily  
24 names, Social Security numbers, birth dates, addresses and, in some instances, driver's license  
25 numbers were breached, in addition to credit card numbers for approximately  
26

1 209,000 U.S. consumers, and certain dispute documents with credit and other personal identifying  
2 information for approximately 182,000 U.S. consumers.

3  
4 61. Since the breach, sources have reported that personal identifying information  
5 accessed during the breach, including addresses, social security numbers, dates of birth and driver  
6 license numbers for various celebrities and public figures are presently offered for sale on the  
7 “Dark Web.”

8  
9 62. The Dark Web is a portion of the internet that is not accessible with traditional web  
10 browsers or through conventional search engines, but allows users with the proper system  
11 configuration to anonymously browse hidden websites and communicate with each other via highly  
12 encrypted messaging protocols.

13  
14 63. While the Dark Web and its associated “TOR” browser technology is widely used  
15 by criminals to traffic in various categories of illicit materials, including drugs, firearms,  
16 professional hitman services, child pornography, and now apparently the private financial  
17 information of most of the adult population of the United States of America previously maintained  
18 by Equifax.

19  
20 64. On September 20, 2017, Comodo Threat Intelligence Labs reported its findings that  
21 the individuals that breached Equifax’s system also injected malware into the system that was  
22 successful in obtaining the login names and passwords of the highest executives at Equifax.

23  
24 65. Using these credentials, the intruders were also able to exploit other services used  
25 by Equifax, such as Dropbox and LinkedIn.

1           66. After obtaining the stolen credentials on the Dark Web and reviewing them,  
2 Comodo found that Equifax's chief privacy officer, chief information officer, vice president of  
3 public relations, and vice president of sales used passwords with major security deficiencies such  
4 as all lowercase letters, no special symbols, and easily guessable words like spouses' names, city  
5 names, and even combinations of initials and birth years.  
6

7  
8                   **Equifax Refuses to Disclose the Fraudulent Procurement of Consumer Files**

9           67. Despite knowing about the breach in July, Equifax kept the information secret. It  
10 did not reveal to individual consumers to whom it owed a contractual duty under a credit  
11 monitoring service. And it did not reveal to the public—those whose information was stolen and  
12 who stand to be injured from the breach—that the breach took place until September 8, 2017. But  
13 even then, Equifax has not disclosed exactly who was affected and what information was accessed.  
14 In the wake of the breach, Equifax's Chief Information Officer and Chief Security Officer have  
15 "retired."  
16

17           68. The credit report information fraudulently procured from Equifax is all that is  
18 necessary to fraudulently obtain credit, tax returns and even a driver's license. With this  
19 information, an identity thief can now open credit, obtain full credit files from other CRAs, and  
20 even verify the falsified identity in future transactions.  
21

22           69. Plaintiffs and class members will incur costs associated with time spent and the loss  
23 of productivity from addressing and attempting to ameliorate, mitigate, and deal with the actual  
24 and future consequences of the Data Breach, including finding fraudulent charges, cancelling and  
25 reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of  
26

1 withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance  
2 of dealing with all issues resulting from the Data Breach; as well as damages to and diminution in  
3 value of their personal and financial information entrusted to Equifax.  
4

5 70. And Equifax knows this, as well as the urgency of providing detailed information  
6 to victim consumers as soon as possible. It warns on its marketing site, “More than ever before,  
7 your employees and customers are at great risk for identity theft and fraud. Over 165 million data  
8 records of U.S. residents have been exposed due to data breaches since January 2005 - Privacy  
9 Rights Clearinghouse.”<sup>5</sup>  
10

11 71. Defendants (now ironically) boast of how effective and robust its data breach  
12 response time and program is, stating, “You’ll feel safer with Equifax. We’re the leading provider  
13 of data breach services, serving more than 500 organizations with security breach events every  
14 day. In addition to extensive experience, Equifax has the most comprehensive set of identity theft  
15 products and customer service coverage in the market.” *Id.* Such “industry leading” services and  
16 capabilities would, by Equifax’s suggestion require the breached business to, “Quickly inform  
17 consumers[.]” *Id.*  
18

19 72. Equifax has, however, not “quickly informed consumers” as to its own data breach.  
20 As of the date of this filing, Equifax still refused to substantively inform affected consumers. And  
21  
22  
23  
24

---

25  
26 5 <http://www.equifax.com/help/data-breach-solutions/> (last visited September 21, 2017).  
27  
28

1 Equifax waited at least six weeks before it publicly disclosed even the general fact of the data  
2 breach.  
3

4 73. Customers who called the dedicated call center set up by Equifax were often unable  
5 to get a coherent or timely response.

6 74. Even the “free” credit monitoring it offered to hack victims came with a string. The  
7 Terms of Service for TrustedID (an Equifax owned company) contain a provision that an  
8 individual’s “membership subscription may be subject to automatic renewal.”<sup>6</sup> Offering credit  
9 monitoring to every American through TrustedID also positions Equifax to collect even more  
10 valuable PII. To sign up, a consumer must authorize TrustedID to retrieve information about the  
11 consumer from the other two credit bureaus (Equifax and TransUnion). The information on the  
12 credit reports of the bureaus can vary by up to 20%, meaning Equifax can gain access to, and  
13 ultimately profit from, additional information from the other two credit bureaus when consumers  
14 grant TrustedID access to their Equifax and TransUnion credit files. It has also been reported that  
15 consumers that accessed the online system were also exposed to a virus.  
16  
17

18 75. The system Defendants implemented to update consumers about whether their  
19 credit reporting information had been procured by the identity thieves was ineffective and not  
20 helpful. To take advantage of this look up, all you need to do is provide your last name and last  
21 six (not 4) digits of your Social Security number. However, the website that Equifax launched  
22  
23  
24  
25

---

26 6 <https://www.trustedid.com/serviceterms.php?serviceterms> (last visited Sept. 21, 2017).  
27  
28

1 often returned the same message to a user regardless of what information was put in.<sup>7</sup> And, the  
2 site is not hosted on the Equifax network and appears to be a website domain and structure that  
3 was previously recognized as critically vulnerable to a hack. Since trust is critical for web sites  
4 like this, especially after a breach of this severity, it is difficult for consumers to trust that Equifax  
5 latest online support option is properly protecting their data.  
6

7 76. Regardless, even assuming the class members did not suffer a false positive;  
8 Equifax has still refused to provide any detailed information as to what specific data was procured  
9 for individual consumers. And the generalized summary of the fact that they produced data  
10 including personal identifying information and some credit card account numbers is of little  
11 comfort to Plaintiffs and class members. What specific documents or files were procured  
12 containing such information? What additional parts of the credit report file was obtained? Which  
13 database(s) were hacked and thus procured? What information does Equifax have as to who  
14 procured it?  
15  
16

17  
18 **COUNT I: BREACH OF DUTY OF CARE**  
19 ***Class Action Claim***

20 77. Plaintiffs restate each of the allegations in the preceding paragraphs as if set forth  
21 at length herein.  
22

23  
24  
25  
26 <sup>7</sup> <https://www.riskbasedsecurity.com/2017/09/equifd-equifax-breach-response-off-to-a-rough-start/> (last visited September 21, 2017).  
27

1           78. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs brings this  
2 action for themselves and on behalf of a class (the “National Breach Class”) defined as:  
3

4                   All natural persons residing in the United States (including all  
5 territories and other political subdivision) whose consumer reporting information  
6 at Equifax was procured as a result of the data breach announced by Equifax on or  
7 about September 7, 2017.  
8

9                   The Class does not include Defendant’s officers, directors, and  
10 employees; Defendant’s attorneys; Plaintiffs’ attorneys; any Judge overseeing or  
11 considering this action together with members of their immediate family and any  
12 judicial staff.  
13  
14

15           79. In addition, Plaintiffs allege a subclass limited to members of the National Breach  
16 Class for whom Defendant’s records show that the primary address of that consumer as of May 1,  
17 2017 was in Arizona.  
18

19           80. The class and subclass, which each number above 100,000 consumers are so  
20 numerous that joinder of all members is impractical.  
21

22           81. There are questions of law and fact common to the class, which common issues  
23 predominate over any issues involving only individual class members. For example, and without  
24 limitation: (a.) whether Equifax had a duty of care to maintain the security of class member credit  
25  
26  
27  
28

1 reporting information; (b.) whether Equifax's duty was heightened; and (c.) whether Equifax  
2 breached that duty in its failure to secure class member data.

3  
4 82. Plaintiffs' claims are typical of those of the class members. All are based on the  
5 same facts and legal theories. The tort alleged is the same and the class claim will rise and fall  
6 entirely based upon whether or not Plaintiffs' claim rises or falls.

7  
8 83. The Plaintiffs will fairly and adequately protect the interests of the class. The  
9 Plaintiffs have retained counsel experienced in handling class actions and litigation against  
10 Equifax as well as involving consumer credit reporting data and privacy protections. Neither  
11 Plaintiffs nor their counsel have any interests that might cause them not to vigorously pursue this  
12 action. The Plaintiffs are aware of their responsibilities to the putative classes and have accepted  
13 such responsibilities.

14  
15 84. Certification of a class under Rule 23(b)(1) of the Federal Rules of Civil Procedure  
16 is proper. Prosecuting separate actions by or against individual class members would create a risk  
17 of adjudications with respect to individual class members that, as a practical matter, would be  
18 dispositive of the interests of the other members not parties to the individual adjudications or would  
19 substantially impair or impede their ability to protect their interests.

20  
21 85. Certification of a class under Rule 23(b)(2) of the Federal Rules of Civil Procedure  
22 is appropriate in that Equifax has acted on grounds generally applicable to the class thereby making  
23 appropriate declaratory relief with respect to the class as a whole.

24  
25 86. Certification of the class under Rule 23(b)(3) of the Federal Rules of Civil  
26 Procedure is also appropriate in that:

1           a.       As alleged above, the questions of law or fact common to the members of the  
2 classes predominate over any questions affecting an individual member. Each of the common  
3 facts and legal questions in the case overwhelm the more modest individual damages issues.  
4 Further, those individual issues that do exist can be effectively streamlined and resolved in a  
5 manner that minimizes the individual complexities and differences in proof in the case.  
6

7           b.       A class action is superior to other available methods for the fair and efficient  
8 adjudication of the controversy. Consumer claims generally are ideal for class treatment as they  
9 involve many, if not most, consumers who are otherwise disempowered and unable to afford and  
10 bring such claims individually. Further, most consumers affected by Equifax's tortious conduct  
11 would likely be unaware of their rights under the law, or who they could find to represent them in  
12 federal litigation. Additionally, individual litigation of the uniform issues in this case would be a  
13 waste of judicial resources. The issues at the core of this case are class wide and should be resolved  
14 at one time. One win for one consumer would set the law as for every similarly situated consumer.  
15

16           87.     Equifax knew or should have known the risks inherent to its possession of massive  
17 amounts of sensitive personal information, including that (a) hackers would target Equifax, as a  
18 dominant player in the consumer credit reporting and data aggregation industry, in order to acquire  
19 such information; (b) the risk of sophisticated cyberattacks was continual and increasing; (c) its  
20 own lax protocols had resulted in prior data breaches; (d) measures were available to adequately  
21 address its cybersecurity deficiencies; and (e) failure to implement adequate cybersecurity  
22 practices would result in a data breach.  
23  
24  
25  
26  
27  
28

1           88.     Equifax's conduct in failing to protect Class Members' information, as described  
2 above, constitutes negligence. Equifax had a duty to act as would a reasonable CRA to safeguard  
3 the personal financial information of consumers entrusted to it by federal and state statutes.  
4 Equifax breached that duty by failing to secure its systems, including but limited to, applying a  
5 simple security patch that had been released for months prior to the break-in, then failing for  
6 months to notify class members that their information was compromised. As a proximate result  
7 of this breach of duty, National Breach Class Members suffered injuries. Those injuries resulted  
8 in monetary damages to Plaintiffs and Class Members.  
9

10  
11           89.     Equifax breached its duties to Plaintiffs and the Class through its conduct alleged  
12 herein. Equifax had the ability to protect Class Members' PII from the cyberattack resulting in the  
13 Data Breach, but failed to do so. Equifax failed to implement reasonable or adequate data security  
14 practices to protect the type and scale of information in its possession, failed to timely detect the  
15 cyberattack, utilized outdated and otherwise improper security measures and techniques, failed to  
16 properly segment and patch systems containing sensitive consumer data, failed to disclose the  
17 flaws in its data security, and failed to provide timely notice of the Data Breach.  
18

19           90.     Equifax would have been able to prevent and/or limit the harm caused by the Data  
20 Breach had it maintained adequate protocols and security measures as alleged herein.  
21

22           91.     Defendants are also strictly liable for the data breach as Equifax owed a duty  
23 because of the uniquely heightened and financially dangerous nature of its business and business  
24 practices.  
25  
26  
27  
28

1           92. Plaintiffs and each class member has suffered actual harm and actual damages as a  
2 result of this breach, for which Plaintiffs seek remedy and judgment.  
3

4                       **WHEREFORE**, Plaintiffs demand judgment and relief as pled and as  
5 follows:

6           A. That an order be entered certifying the proposed Classes under Rule 23 of the  
7 Federal Rules of Civil Procedure and appointing Plaintiffs and their counsel to represent them;

8           B. That judgment be entered against Defendants as pled for actual, statutory, treble  
9 and punitive damages;  
10

11           C. That the Court award costs and reasonable attorney's fees, pursuant to 15 U.S.C.  
12 §§ 1681o and n;

13           D. That the Court grant disgorgement, rescission and other injunctive and declaratory  
14 relief as pled, and requiring Equifax to make the full disclosures otherwise required to class  
15 members;  
16

17           E. That the Court grant such other and further relief as may be just and proper.

18                       **PLAINTIFFS DEMAND TRIAL BY JURY**

19                                       **Respectfully,**

20                                       **CORINNE COOPER, MORGAN**  
21                                       **RUTHERFORD, DONNA DECONCINI, MARY**  
22                                       **BRADLEY, DEBBIE REINERT, RANDY**  
23                                       **REINERT,**  
24                                       *on behalf of themselves and all others*  
25                                       *similarly situated,*  
26  
27  
28

By: /s/ Susan M. Rotkis

Susan M. Rotkis, AZ Bar 032866  
Consumer Litigation Associates West, PLLC  
382 S. Convent Ave.  
Tucson, AZ 85716  
520-622-2481  
srotkis@clalegal.com

Leonard A. Bennett  
*pro hac vice*  
Consumer Litigation Associates, P.C.  
763 J. Clyde Morris Blvd, Suite 1-A  
Newport News, VA 23601  
757-930-3660  
lenbennett@clalegal.com